Lecture : Thursday, Feb 9th 2012

Talk 2 of Minicourse 3 by Emmanuel Kowalski

Sieve in discrete groups - Part II

Notation : Γ = discrete group, $\Gamma \longrightarrow GL_n(\mathbb{Z})$

$\Gamma \twoheadrightarrow \prod_{p \mid q} \Gamma_p$; q is square free.

$\Gamma \twoheadrightarrow \Gamma_p$ finite. $\quad \left\{ {}^{*}(q, q_0) = 1 \right\}$

$\Omega_p \subset \Gamma_p$

$X = \{ \gamma \in \Gamma \,:\, \gamma \pmod p \notin \Omega_p \,,\ \forall\, p \in P \}$

"Heuristic" $\quad |X \cap B_T| \approx \prod_{p \in P} \left(1 - \frac{|\Omega_p|}{|\Gamma_p|} \right) |B_T|$.

classical : $X \cap \{1, \dots, N\}$.

$P = \{ p \le Q = N^{\beta} \}$, $\beta > 0$.

"Small" sieves

$\frac{|\Omega_p|}{|\Gamma_p|} \approx \frac{K}{p}$, K - fixed, p - prime.

"Large" Sieves (Linnik 1941)

$$1 \geq \frac{|\Omega_p|}{|\Gamma_p|} \geq c > 0, \quad \forall p, \quad c \text{ independent of } p.$$

Remarks: ① one can not expect to get lower bounds on size of X.

Ex:- $\Gamma = \mathbb{Z}$, $\Omega_p = \{\text{non-squares in } \mathbb{Z}/p\mathbb{Z}\}$.

$$\frac{|\Omega_p|}{p} \approx \frac{1}{2}.$$

$X \supset \{\text{squares}\}$.

$|X \cap \{1, \ldots, N\}| \gg N^{1/2}$, whereas heuristics predict much less. (ref: Helfgott - Venkatesh, Walsh)

② The Large Sieve does not know about primes.

Slogan:- the large-sieve gives very useful and general upper bounds for the size of X in balls.

Examples:- (1) $\langle S \rangle = \Gamma \subset SL_n(\mathbb{Z})$.

$\overline{\Gamma}^{zar} = SL_n$.

$f : SL_n(\mathbb{Z}) \longrightarrow \mathbb{Z}$ non-constant.

$\phi : Y \longrightarrow SL_n$, $Y/\mathbb{Q}$: irreducible. quasifinite degree ≥ 2 dominant.

Ex: $\phi : M_n \longrightarrow M_n$
$(a_{ij}) \longmapsto (a_{ij}^2)$.
$\phi^{-1}(SL_n) \xrightarrow{\phi|_{SL_n}} SL_n$
$\phi(Y(\mathbb{Q})) \subset SL_n(\mathbb{Q})$ is called "thin"/"mince"

Know: $\Gamma_{\mathbb{Z}}(f)$ is Zariski-dense in SL_n.

Question: Can it be that $\Gamma_{\mathbb{Z}}(f) \subset \phi(Y(\mathbb{Q}))$?

Answer : No!

- If $\gamma \in \phi(Y(\mathbb{Q}))$ then modulo p.

$\gamma \bmod p \in \phi(Y(\mathbb{F}_p))$

$\gamma \bmod p \notin \Omega_p$ = complement of $\phi(Y(\mathbb{F}_p))$.

one shows $\exists c$ $\dfrac{|\Omega_p|}{|\Gamma|} \geq c > 0$ (Lang-Weil).

$$\{\gamma \in \Gamma \mid \gamma \in \phi(Y(\mathbb{Q}))\} \subset X.$$

One shows: $\exists\, \beta = \beta(Y)$, $\forall N$, $P(Y_N \in X) \ll e^{-\beta N}$

where Y_N - random walk using S.

(Note: For counting problems over finite fields see paper of Chatzidakis - Van den Dries - Macintyre in Crelle titled "Definable sets over finite fields - 1992")

(2) [Rivin, Kowalski, Jowe - Kocoalski - Zywina, Lubotzky - Rosenzoveig].

Splitting field of characteristic polynomials of

$\gamma \in \Gamma \subset GL_n(\mathbb{Z})$.

Assume: $G = \overline{\Gamma}^{zar}$ is connected semisimple.

[e.g.: $G = E_8 \subset GL(248, \mathbb{Z})$]

$\gamma \in \Gamma$, $P_\gamma(T) = \det(T - \gamma) \in \mathbb{Z}[T]$.

Question: what is the typical Galois-group of the splitting field of P_γ?

- Method 3

Theorem: $\exists\, \beta$, $P(Gal(P_{\gamma_N}) \neq W(G)) << e^{-\beta N}$.

Link with Sieve. $\overline{\Gamma}^{zar} = SL_n$, $W(G) = S_n$

Observation (Gallagher) If P_γ is reducible,

$$P_\gamma \pmod p \notin \Omega_p = \{ g \in SL_n(\mathbb{F}_p) : \det(T-g) \text{ is irreducible} \}.$$

$$\frac{|\Omega_p|}{|\Gamma_p|} \underset{p\to\infty}{\sim} \frac{1}{n}, \quad \forall\, p \quad \text{(Chavdarov)}.$$

(3) (Dunfield – Thurston random 3-manifolds)

$g \geq 2$ fixed.

$\langle S \rangle = \Gamma_g$ mapping class-group.

$$\Gamma_g \twoheadrightarrow Sp_{2g}(\mathbb{Z}).$$

Y_N = random walk of length N on Γ_g.

$M_N = Hg \underset{Y_N}{\cup} Hg$ ← handlebody of genus g.

$\dim_{\mathbb{Q}} H_1(M_N, \mathbb{Q}) = ?$

· If $H_1(M_N, \mathbb{Q}) \neq 0$, then $H_1(M_N, \mathbb{F}_p) \neq 0, \forall p$.

(Lagrangian mod $p \simeq \mathbb{F}_p^g$) ← $(Y_N \bmod p) \cdot J_p \cap J_p$ (112)

So, $Y_N \bmod p \notin \Omega_p = \{\gamma \in Sp_{2g}(\mathbb{F}_p) : 1 : \gamma J_p \cap J_p = 0\}$.

Fact: $\dfrac{|\Omega_p|}{|\Gamma_p|} \geq c > 0$.

Theorem: $\exists \beta > 0$, $\mathbb{P}\left(H_1(M_N, \mathbb{Q}) \neq 0\right) \ll e^{-\beta N}$.

Theorem: (Lubotzky – Mesbri)

$\Gamma = \langle S \rangle$, $S = S^{-1}$, $1 \in S$.

Let $N_j = \ker(\Gamma \twoheadrightarrow \Gamma_j)$ where Γ_j is finite, for $j \in J$. Assume:

① $\left(\mathcal{C}(\Gamma_i \backslash \Gamma_j, S \bmod N_j)\right)_{i,j \in J}$ is an expander.

② $|\Gamma_j| \leq j^d$ for some fixed d.

③ $\forall\, i \neq j$, $\Gamma \longrightarrow \Gamma_j \times \Gamma_i$ is onto.

Let $X \subset \Gamma$ such that $\exists\, \delta > 0$, independent j,

④ $|X \bmod N_j| \leq (1-\delta)|\Gamma_j|$

Then, $\exists\, \beta > 0$, $\mathbb{P}(Y_N \in X) \ll e^{-\beta N}$.

- Proof is surprisingly short.
  (R. Peled, Chebychev inequality ...)

- Application :

Theorem (Lubotzky - Meiri)

Let $\Gamma < GL_n(\mathbb{C})$ be finitely generated.
Assume Γ is not virtually solvable then
for any random walk on Γ, Y_N, we have
$\exists\ \beta > 0$ s.t.

$$\mathbb{P}\left(Y_N \in \{\gamma \in \Gamma : |\ \exists\ m \geq 2,\ \gamma' \in \Gamma,\ \gamma = (\gamma')^m\}\right) << e^{-\beta N}.$$

- Remarks :-

① Improvement of work of Hrushovski - Kropholler - Lubotzky - Shalev.

② For m large, one must ($m \gg \log N$) use different ideals to deal with them.

———×———